ON THE EQUIVALENCE OF QUADRATIC FORMS

BY

T. A. SPRINGER

(Communicated by Prof. H. FREUDENTHAL at the meeting of February 28, 1959)

1. In his fundamental paper [6] on the theory of quadratic forms, E. WITT introduced invariants for the equivalence classes of quadratic forms over an arbitrary field. The most important of these invariants are algebra classes. In their construction the Clifford algebra of the quadratic form is an important tool.

In the present paper we shall try to make clear the mechanism underlying the construction of these invariants. Instead of algebra classes, we shall use 2-cohomology classes. In § 2 we show that the equivalence classes of quadratic forms of a given dimension over a given field may be described by the elements of a certain non-commutative Galois 1-cohomology set. Then in § 3 we shall describe how one can obtain, using Clifford algebras, from such a non-commutative 1-cohomology class an ordinary Galois 2-cohomology class. If one analyses how this is done it is seen that the reason why the Clifford algebra is used is that one can obtain from it a 2-cohomology class of the orthogonal group in the multiplicative group of the underlying field. From this 2-cohomology class and the noncommutative 1-cohomology-class one obtains the invariants by algebraic manipulations.

The procedure used in § 3 may be described in a more general way, but we shall not insist on this.

Finally we remark that we have also treated the case of nondefective forms of characteristic 2, obtaining thus results of C. ARF [1].

2. Let E be a vectorspace with dimension $n>1$ over a commutative field K and let Q be a quadratic form on E, i.e. a mapping of E into K such that

$$(2.1)\qquad \begin{cases} Q(\lambda x)=\lambda^2 Q(x) \qquad (\lambda\in K), \\ B(x,y)=Q(x+y)-Q(x)-Q(y) \text{ is a bilinear function on } E\times E. \end{cases}$$

We always assume that the bilinear function B is nondegenerate (which is usually expressed by saying that Q is nondegenerate if the characteristic $\chi(K)$ is not 2, and that Q is nondefective if $\chi(K)=2$).

B being nondegenerate, the discriminant $\Delta(Q)$ is an element of $K^*/(K^*)^2$ if $\chi(K)\neq 2$ and of $K/\mathscr{P}(K)$ if $\chi(K)=2$, $\mathscr{P}$ denoting the mapping of K defined by $\mathscr{P}(\lambda)=\lambda+\lambda^2$ (see [4] for details, we use the name discriminant instead of pseudo-discriminant in the case $\chi(K)=2$). We also denote by $\Delta(Q)$ a representative of the discriminant in K^* or K.

Q_1 and Q_2 being two quadratic forms on E_1 and E_2 respectively, we define a form $Q_1 \dotplus Q_2$ on $E_1 \dotplus E_2$ by

$$(2.2) \qquad (Q_1+Q_2)(x_1, x_2)=Q_1(x_1)+Q_2(x_2).$$

Q_1-Q_2 is defined similarly.

Now let Q be as above, let L be a Galois extension with group $G=G_{L/K}$. We put $E^L=L\otimes E$ (the tensorproduct being taken over K). This is a vectorspace over L. We define a quadratic form Q^L on E^L by

$$(2.3) \qquad Q^L(\sum_{i=1}^n \lambda_i \otimes x_i)=\sum_{i=1}^n \lambda_i^2 Q(x_i)+\sum_{i<j}\lambda_i\lambda_j B(x_i, x_j) \qquad (\lambda_i \in L, x_i \in E).$$

It is easily seen that this definition makes sense. Now σ being a K-automorphism of L, we define a mapping of E^L, also denoted σ, by

$$(2.4) \qquad \sigma(\sum_{i=1}^k \lambda_i \otimes x_i)=\sum_{i=1}^k (\sigma\lambda_i)\otimes x_i$$

Identifying E with the subset $1\otimes E$ of E^L, E consists of the $x\in E^L$ with $\sigma x=x$.

Further, φ being a mapping of E^L into L (or E^L) we define $\sigma\varphi$ by

$$(2.5) \qquad (\sigma\varphi)(x)=\sigma(\varphi(\sigma^{-1}x))$$

Then

$$(2.6) \qquad (\sigma\tau)(\varphi)=\sigma(\tau\varphi).$$

Q^L being as in (2.3), it follows that

$$(2.7) \qquad \sigma(Q^L)=Q^L$$

for any $\sigma\in G$.

Conversely, let Q' be a quadratic form on E^L such that $\sigma Q'=Q'$ for all $\sigma\in G$, then it is readily seen that $Q'=Q^L$, where Q is a quadratic form on E, uniquely determined by Q'. A similar result holds for linear transformation of E^L.

Now let Q and Q_1 be two quadratic forms on the vector space E over K. They are called equivalent if there is an automorphism t of E such that

$$Q_1(x)=Q(t(x)).$$

We wish to find criteria for the equivalence of two quadratic forms Q and Q_1. For this purpose we shall extend the field K such that Q and Q_1 become equivalent in the extended field and then try to descend again to K.

Lemma 2.1. *There is a Galois extension L of K of finite degree such that Q^L and Q_1^L are equivalent.*

Proof: a) $\chi(K) \neq 2$. We can find bases (e_i), (f_i) of E such that

$$Q(\sum_1^n \xi_i e_i) = \sum_1^n \alpha_i \xi_i^2, \; Q_1(\sum_1^n \xi_i f_i) = \sum_1^n \beta_i \xi_i^2.$$

We may take for L the field generated by the square roots of all $\alpha_i \beta_i$ $(1 \leqslant i \leqslant n)$. b) $\chi(K) = 2$. Our assumption of nondegeneracy of the bilinear forms implies that n is even $= 2m$ and that we can find bases (e_i), (f_i) of E such that

$$Q(\sum_1^n \xi_i e_i) = \sum_1^m (\alpha_i \xi_i^2 + \beta_i \xi_i \xi_{i+m} + \gamma_i \xi_{i+m}^2),$$

$$Q_1(\sum_1^n \xi_i f_i) = \sum_1^m (\lambda_i \xi_i^2 + \mu_i \xi_i \xi_{i+m} + \nu_i \xi_{i+m}^2),$$

where $\beta_i \neq 0$, $\mu_i \neq 0$ (see [4]). We may now take for L the field generated by the roots of the (separable) polynomials $\alpha_i T^2 + \beta_i T + \gamma_i$, $\lambda_i T^2 + \mu_i T + \nu_i$ $(1 \leqslant i \leqslant m)$.

If Q, Q_1 and L have the property of the lemma, we shall say that Q and Q_1 are *L-equivalent*. Now if this is so, there exists a linear transformation t of E^L such that

$$Q_1^L(x) = Q^L(t(x)) \qquad (x \in E^L).$$

By (2.7) we have $\sigma Q^L = Q^L$, $\sigma Q_1^L = Q_1^L$ for all σ in the Galoisgroup G, hence by (2.5)

$$Q^L(t(x)) = Q_1^L(x) = (\sigma Q_1^L)(x) = \sigma(Q_1^L(\sigma^{-1}x)) = \sigma(Q^L(t(\sigma^{-1}(x)))) =$$
$$= (\sigma Q^L)((\sigma t)(x)) = Q^L(\sigma t(x)).$$

Now σt is again a linear transformation of E^L, and we have

$$\sigma t = u_\sigma t, \tag{2.8}$$

where u_σ is an *orthogonal transformation* of Q^L. (2.6) implies at once that

$$u_{\sigma\tau} = \sigma u_\tau \cdot u_\sigma \qquad (\sigma, \tau \in G). \tag{2.9}$$

The linear transformation t of (2.8) is not unique, but the only possible changement is a replacement of t by $u^{-1}t$ (u orthogonal), which changes u_σ into

$$u'_\sigma = (\sigma u)\, u_\sigma u^{-1}. \tag{2.10}$$

Now let $O(L) = O(Q, L)$ be the orthogonal group of Q^L. Defining as usual the cohomology set $H^1(L, Q)$ as the set of equivalence classes of the cocycles u_σ (satisfying (2.9)) under the equivalence relation given by (2.10), we see that a Q_1 which is L-equivalent to Q gives rise to an element $c_L(Q, Q_1)$ of $H^1(L, Q)$. It is easily seen that $c_L(Q, Q_1)$ equals the "neutral" element ε of $H^1(L, Q)$, given by $u_\sigma = 1$, if and only if Q and Q_1 are already K-equivalent.

Now let Q_1 and Q_2 be quadratic forms, which are both L-equivalent to Q. Suppose that $c_L(Q, Q_1) = c_L(Q, Q_2)$. We have $Q_i(x) = Q(t_i(x)) (i = 1, 2)$, where t_1, t_2 are automorphisms of E^L. They may be chosen such that $\sigma t_1 = u_\sigma t_1$, $\sigma t_2 = u_\sigma t_2$, where u_σ is a representative of the class $c_L(Q, Q_1)$. Hence $\sigma(t_2^{-1} t_1) = t_2^{-1} t_1$, which implies that $t_1 = t_2 t^L$, where t^L is the extension to E^L of a linear transformation of E. Then $Q_2(t^L(x)) = Q_1(x) (x \in E^L)$. For $x \in E$ this gives $Q_2(t(x)) = Q_1(x)$, i.e. Q_1 and Q_2 are equivalent. Conversely, if Q_1 and Q_2 are equivalent, and if both are L-equivalent to Q then $c_L(Q, Q_1) = c_L(Q, Q_2)$.

Finally, if c is an arbitrary element of $H^1(L, Q)$, we take a cocycle (u_σ) representing c. By a theorem of Speiser (see appendix) there is a non-singular linear transformation t of E^L such that (2.8) holds. Putting $Q'(x) = Q^L(t(x)) (x \in E^L)$, (2.8) implies that $\sigma Q' = Q'$, hence $Q' = Q_1^L$, where Q_1 is a quadratic form on E.

Collecting these results we find

Theorem 2.1. *The equivalence classes of quadratic forms Q_1 on E which are L-equivalent to Q are in $1-1$-correspondence with the elements of $H^1(L, Q)$. The class of Q corresponds to the neutral element.*

This result may be generalized for infinite extensions L in a well-known manner. We must give the Galoisgroup of L over K the Krull topology, $O(Q, L)$ the discrete topology, and we consider only continuous (u_σ). In this way we find

Theorem 2.2. *Let Ω be the separable algebraic closure of K. The equivalence classes of n-dimensional quadratic forms over K are in $1-1$-correspondence with the elements of $H^1(\Omega, Q)$, where Q is a particular n-dim. quadratic form.*

We add the following remark in the case $\chi(K) \neq 2$. If Q and Q_1 have the same discriminant, then it is readily verified that the determinant of t is in K, hence that the determinant of u_σ is 1. Defining $H^1_+(L, Q)$ to be the cohomology set defined by cocycles in the rotation group $O^+(Q, L)$, we find

Theorem 2.3. *The equivalence classes of quadratic forms Q_1 on E which are L-equivalent to Q and have the same discriminant as Q are in $1-1$-correspondence with the elements of $H^1_+(L, Q)$.*

If $\chi(K) = 2$ and Q is nondefective, theorem 2.3 remains true, the proof carries over to that case with appropriate modifications.

3. We have obtained above a description of the equivalence classes of quadratic forms in terms of non-commutative 1-cohomology sets. Not much information is available about the latter, hence it is preferable to pass to commutative cohomology groups. We shall show how this may be done in the case under consideration.

Let Q be as above. We need the Clifford algebra $C(Q)$ of Q. We recall its definition: let T be the tensoralgebra of E, let I be the twosided ideal in T generated by the elements $x \otimes x - Q(x)$, then $C = T/I$. E may be identified with a subspace of C. We call even (odd) the elements of C which are linear combination of the images in C of homogeneous tensors of even (odd) degree. The even elements of $C(Q)$ form a subalgebra $C^+ = C^+(Q)$, the second Clifford algebra of Q. The odd elements form a complementary subspace of C^+ in C. We define a function η by

$$\eta(x) = \begin{cases} 1 & \text{if } x \text{ is even} \\ -1 & \text{if } x \text{ is odd.} \end{cases} \tag{3.1}$$

We also put $\varepsilon(x) = 0$ if x is even and $\varepsilon(x) = 1$ if x is odd. Hence $\eta(x) = (-1)^{\varepsilon(x)}$ if x is even or odd.

Moreover we denote by $x \to \tilde{x}$ the involution in C obtained from the transformation $x_1 \otimes \ldots \otimes x_p \to x_p \otimes \ldots \otimes x_1$ in T.

We have to use the following result.

Lemma 3.1. *If Q is a quadratic form on E then to any orthogonal transformation t of Q corresponds an invertible element s_t of C so that*

$$t(x) = d(t)\, s_t x s_t^{-1} \qquad (x \in E), \tag{3.2}$$

where $d(t)$ is the determinant of t (hence ± 1). If $\chi(K) = 2$, then s_t is determined up to a factor in K^* by these conditions, if $\chi(K) \neq 2$ this is true provided we require s_t to be even (odd) if $d(t) = 1(-1)$. Hence $d(t) = \eta(s_t)$ in the last case.

For a proof see [4]. In applying this lemma we always assume that s_t is either even or odd.

It follows at once from (3.2) that we have

$$s_{tu} = \gamma(t, u)\, s_t s_u, \tag{3.3}$$

where $\gamma(t, u) \in K^*$ is a 2-cocycle of the orthogonal group $O(Q)$ in K^*, operating trivially on K^*. Moreover, since s_t is determined up to a factor in K^*, we find a cohomology class γ in the 2-cohomology group $H^2(Q, K^*)$ of $O(Q)$ in K^*.

Now let L be a finite dimensional Galois extension of K with group G. Then we may identify the Clifford algebra $C(Q^L)$ with $L \otimes C(Q)$. Hence G operates on $C(Q^L)$.

Lemma 3.2. *We may take the s_t of lemma 3.1 such that*

$$s_{\sigma t} = \sigma(s_t) \tag{3.4}$$

for all orthogonal transformations t of Q^L and all $\sigma \in G$.

Proof: If $t(x) = d(t)\, s_t x s_t^{-1} (x \in E^L)$, then

$$(\sigma t)(x) = \sigma(t(\sigma^{-1} x)) = d(\sigma t)\, \sigma s_t\, x (\sigma s_t)^{-1}.$$

Hence $\sigma s_t = x_{\sigma,t} s_{\sigma t}$, $(x_{\sigma,t} \in L^*)$ which implies

$$\alpha_{\sigma\tau,t} = \alpha_{\sigma,\tau t}\,\sigma(\alpha_{\tau,t}). \tag{3.5}$$

Because of the linear independence of the automorphisms $\sigma \in G$, there is an element $\lambda \in L$, such that

$$\alpha_t = \sum_{\tau \in G} \alpha_{\tau,\tau^{-1}t}\,\tau\lambda \neq 0.$$

It follows, using (3.5), that

$$\sigma\alpha_t = \alpha_{\sigma,t}^{-1}\,\alpha_{\sigma t},$$

where

$$\alpha_{\sigma t} = \sum_{\tau \in G} \alpha_{\tau,\tau^{-1}\sigma t}\cdot\tau\lambda.$$

Hence

$$\alpha_{\sigma t} \neq 0, \text{ and } \sigma(\alpha_t s_t) = \alpha_{\sigma t} s_{\sigma t}.$$

Replacing $s_{\sigma t}$ by $\alpha_{\sigma t}\cdot s_{\sigma t}(\sigma \in G)$ we find that for a given t we may take the $s_{\sigma t}$ such that $s_{\sigma t} = \sigma(s_t)$. We obtain the assertion of lemma 3.2 by decomposing the set of all t in transitivity classes under G.

As explained above, we can find a 2-cohomology class γ_L in $H^2(Q^L, L^*)$, for which we also write $H^2(Q, L^*)$. Lemma (3.2) implies, that γ_L contains an "equivariant" cocycle $\gamma(t, u)$, which satisfies

$$\gamma(\sigma t, \sigma u) = \sigma(\gamma(t, u)). \tag{3.6}$$

Now let $a \in H^1(L, Q)$, take a cocycle (u_σ) in a. We can find elements s_{u_σ} in $G(Q^L)$ such that

$$u_\sigma(x) = d(u_\sigma)\, s_{u_\sigma} x\, s_{u_\sigma}^{-1} \qquad (x \in E^L,\ \sigma \in G),$$

and such that

$$s_{\sigma u_\tau} = \sigma s_{u_\tau}.$$

Put

$$\alpha(\sigma, \tau) = \gamma(\sigma u_\tau, u_\sigma) = s_{u_{\sigma\tau}}\, s_{u_\sigma}^{-1}\, \sigma(s_{u_\tau}^{-1}). \tag{3.7}$$

where γ is a cocycle in γ_L satisfying (3.6).

It follows that α is a 2-cocycle of G in L^* (G operating in the natural way). Moreover it is readily verified that α varies by a coboundary if (u_σ) varies in its cohomology class. Denoting by $H^2(L)$ the Galois cohomology group, we have found a mapping

$$\varphi\colon H^1(L, Q) \to H^2(L).$$

Now $c_L(Q, Q_1)$ being as in nr. 2, we define $a_L(Q, Q_1) \in H^2(L)$ by

$$a_L(Q, Q_1) = \varphi(c_L(Q, Q_1)). \tag{3.8}$$

4. Theorem 2.1 implies

Theorem 4.1. *If Q and Q_1 are equivalent, then $a_L(Q, Q_1) = 1$ for all L.*

The converse of theorem 4.1 does not hold, however we can prove the following result.

Theorem 4.2. *Suppose that Q and Q_1 are L-equivalent for some Galois extension L of K. If $\Delta(Q)=\Delta(Q_1)$, $a_L(Q, Q_1)=1$, then the Clifford algebra's $C(Q)$ and $C(Q_1)$ are isomorphic. The same is true of the algebra's $C^+(Q)$ and $C^+(Q_1)$.*

Proof. If $\Delta(Q)=\Delta(Q_1)$, the u_σ of a cocycle of $c_L(Q, Q_1)$ are rotations. Moreover, using the above notations, if $a_L(Q, Q_1)=1$, we may take the $\alpha(\sigma, \tau)$ to be 1. Hence we have

$$s_{u_{\sigma\tau}} = \sigma s_{u_\tau} s_{u_\sigma}.$$

Then there is a nonsingular s in C^L such that $s_{u_\sigma}=\sigma s \cdot s^{-1}$ (see appendix). This gives

$$u_\sigma(x) = (\sigma s)s^{-1} xs(\sigma s)^{-1},$$

but if $u_\sigma=\sigma t \cdot t^{-1}$, $Q_1^L(x)=Q^L(t(x))$, we obtain

$$(\sigma s)^{-1}((\sigma t)x)(\sigma s) = s^{-1} t(x) s \qquad (x \in E^L) \tag{4.1}$$

Now put for $x \in E^L$

$$\psi(x) = s^{-1} t(x) s,$$

then by (4.1) we have $\sigma\psi=\psi(\sigma \in G)$.

Further if $x \in E^L$, we have $\psi^2(x)=s^{-1}t^2(x)s=Q^L(t(x))=Q_1(x)$.

Now if C_1^L is the Clifford algebra of Q_1^L, there is a homomorphism ψ' of C^L into C_1^L, defined by

$$\psi'(x) = \psi(x) \qquad (x \in E^L)$$

(see [3], p. 39). Since E^L generates C^L, the $\psi'(x)$ $(x \in E^L)$ generate C^L, hence ψ' is onto and since the dimensions of C^L and C_1^L are equal, ψ is an isomorphism. Since $\sigma\psi=\psi$, we have $\sigma\psi'=\psi'(\sigma \in G)$. Thus if $x \in C_1^L$, $\sigma x = x$, we have $\sigma(\psi'(x)=\psi'(x)$. Since $C(Q)$ $(C(Q_1))$ consists of the elements of $C^L(C_1^L)$ invariant under all $\sigma \in G$, ψ' induces an isomorphism of $C(Q)$ and $C(Q_1)$. The result for $C^+(Q)$ and $C^+(Q_1)$ follows easily.

We proceed by proving a few properties of the cohomology classes $a_L(Q, Q_1)$.

Theorem 4.3. *$a_L(Q, Q_1)$ has order 1 or 2.*

Proof. It is well-known (see [4]) that the elements s_t of (3.2) satisfy $s_t\bar{s}_t \in K^*$ (where $\bar{s}_t$ is the transform of s_t under the involution in C), using this for the s_{u_σ} we find at once from (3.7) that $\alpha(\sigma, \tau)$ is a coboundary.

In order to formulate the next theorem we need a special cohomology class. We assume $\chi(K)\neq 2$. Let $\alpha, \beta \in K^*$, assume that the Galois extension L of K contains square roots $\lambda(\mu)$ of $\alpha(\beta)$. Then for any σ in the group G of L over K we have $\sigma\lambda=(-1)^{\alpha(\sigma)}\lambda$, $\sigma\mu=(-1)^{\beta(\sigma)}\mu$, where $\alpha(\sigma)$, $\beta(\sigma)$ are integers (determined mod 2). Then we define a cohomology class $(\alpha, \beta) \in H^2(L)$ as the class of the cocyle f with

$$f(\sigma, \tau) = (-1)^{\alpha(\sigma)\beta(\tau)},$$

hence $f(\sigma, \tau) = -1$ if $\sigma\lambda = -\lambda$, $\sigma\mu = -\mu$ and $f(\sigma, \tau) = 1$ in all other cases (it is readily verified that f is a cocycle). Of course (α, β) depends on L, but it is well-known that if M is a larger Galois extension of K, then the lift of L to M of (α, β) is the class (α, β) of $H^2(M)$. We could also define (α, β) as an element of $H^2(\Omega)$, Ω being the separable algebraic closure of K. It follows easily from the definition that (α, β) is symmetric in α and β, and multiplicative in α and β.

Theorem 4.4. *If Q, Q_1, Q_2 are three quadratic forms on E, then*

$$a_L(Q_1, Q_2) = (\Delta(Q)\Delta(Q_1), \Delta(Q_1)\Delta(Q_2))\, a_L(Q, Q_1)\, a_L(Q, Q_2) \quad \text{if } \chi(K) \neq 2,$$

and

$$a_L(Q_1, Q_2) = a_L(Q, Q_1)\, a_L(Q, Q_2) \quad \text{if } \chi(K) = 2.$$

($\Delta(Q)$, ... denote representatives of the discriminant of Q, ...).

Proof. Take automorphisms t_i of E^L such that $Q_i^L(x) = Q^L(t_i(x))$ ($x \in E^L$, $i = 1, 2$).

Then $Q_2^L(x) = Q_1^L(t_1^{-1}t_2(x))$. Let $\sigma t_1 = u_\sigma t_1$, $\sigma t_2 = v_\sigma t_2 (u_\sigma, v_\sigma \in O(Q_1^L))$. Then $\sigma(t_1^{-1}t_2) = w_\sigma(t_1^{-1}t_2)$, where $w_\sigma = t_1^{-1}(u_\sigma^{-1}v_\sigma)t_1 \in O(Q_1^L)$.

Now since $Q^L(t_1(x)) = Q_1^L(x)$, the automorphism t_1 of E^L may be extended to an isomorphism θ of $C^L(Q_1)$ onto $C^L(Q)$ (as in the proof of Th. 4.2), such that $\theta(x) = t_1(x)$ if $x \in E^L$. Assume first $\chi(K) \neq 2$.

Lest s_{u_σ}, s_{v_σ} be elements of $C^L(Q)$ with

$$u_\sigma(x) = d(u_\sigma)s_{u_\sigma}x\, s_{u_\sigma}^{-1}$$

$$v_\sigma(x) = d(v_\sigma)s_{v_\sigma}x\, s_{v_\sigma}^{-1}$$

By lemma 3.1 we have

$$d(u_\sigma) = \eta(s_{u_\sigma}),\quad d(v_\sigma) = \eta(s_{v_\sigma}) \qquad (\eta \text{ being defined by (3.1)}).$$

We have in $C^L(Q_1)$

$$w_\sigma(x) = d(w_\sigma)s_{w_\sigma}x\, s_{w_\sigma}^{-1} \qquad (x \in E^L),$$

with

$$s_{w_\sigma} = \theta^{-1}(s_{u_\sigma}^{-1}\, s_{v_\sigma}).$$

Now if $x \in E^L$ we have

$$(\sigma\theta)(x) = (\sigma t_1)(x) = u_\sigma t_1(x) = d(u_\sigma)s_{u_\sigma}t_1(x)s_{u_\sigma}^{-1} = d(u_\sigma)s_{u_\sigma}\theta(x)s_{u_\sigma}^{-1}.$$

It follows that for $x \in C^L(Q_1)$ we have

$$(\sigma\theta)(x) = (d(u_\sigma))^{\varepsilon(x)}\, s_{u_\sigma}\theta(x)s_{w_\sigma}^{-1},$$

if x is either even or odd (ε is defined by $\eta(x) = (-1)^{\varepsilon(x)}$).

Now

$$\sigma s_{u_\tau}^{-1} \cdot \sigma s_{v_\tau} = \sigma(\theta(s_{w_\tau})) = (d(u_\sigma))^{\delta(w_\tau)}\, s_{u_\sigma}\theta(\sigma s_{w_\tau})s_{u_\sigma}^{-1},$$

where

$$d(w_\tau) = (-1)^{\delta(w_\tau)}.$$

This gives
$$\theta(\sigma s_{w_\tau}) = (d(u_\sigma))^{\delta(w_\tau)} s_{u_\sigma}^{-1} (\sigma s_{u_\tau}^{-1} \cdot \sigma s_{v_\tau}) s_{u_\sigma},$$
whence
$$\theta(\sigma s_{w_\tau} \cdot s_{w_\sigma}) = (d(u_\sigma))^{\delta(w_\tau)}\, s_{u_\sigma}^{-1}\, \sigma s_{u_\tau}^{-1}\, \sigma s_{v_\tau}\, s_{v_\sigma},$$
giving finally
$$s_{w_{\sigma\tau}} = \varrho(\sigma, \tau)\, \sigma s_{w_\tau} \cdot s_{w_\sigma},$$

with $\varrho(\sigma,\tau) = \gamma^{-1}(\sigma,\tau)\,\gamma_1(\sigma,\tau)\,\lambda(\sigma,\tau)$, where the cocyles $\gamma, \gamma_1, \lambda$ are defined by
$$s_{u_{\sigma\tau}} = \gamma(\sigma,\tau)\, \sigma s_{u_\tau}\, s_{u_\sigma}, \quad s_{v_{\sigma\tau}} = \gamma_1(\sigma,\tau)\, \sigma s_{v_\tau}\, s_{v_\sigma},$$
and
$$\lambda(\sigma,\tau) = (d(u_\sigma))^{\delta(w_\tau)}.$$

Now $\lambda(\sigma,\tau) = 1$ unless $d(u_\sigma) = -1$, $d(w_\tau) = -1$. Hence $\lambda(\sigma,\tau) = \pm 1$ and $+1$ unless $\sigma(dd_1) = -dd_1$, $\sigma(d_1, d_2) = -d_1 d_2$, where d, d_i are such that $d^2 = \Delta(Q), d_i^2 = \Delta(Q_i)$ $(i = 1, 2)$.

This implies the theorem for $\chi(K) \neq 2$. If $\chi(K) = 2$ the argument is similar, only somewhat simpler since the $d(u_\sigma)$ are all 1 in this case.

Corollary. *$a_L(Q, Q_1)$, if defined, depends only on the equivalence classes of Q and Q_1.*

Proof. If Q is equivalent to Q_1, then $\Delta(Q) = \Delta(Q_1)$, $a_L(Q, Q_1) = 1$, hence $a_L(Q, Q_2) = a_L(Q_1, Q_2)$ for all Q_2. If Q_1 is equivalent to Q_2, then we obtain similarly $a_L(Q, Q_1) = a_L(Q, Q_2)$.

Theorem 4.5. *If Q, Q_i are L-equivalent $(i = 1, 2)$, if $\Delta(Q_1) = \Delta(Q_2)$, $a_L(Q, Q_1) = a_L(Q, Q_2)$, then the Clifford algebra's of Q_1, Q_2 are isomorphic. The same is true for the second Clifford algebra's.*

Proof. By theorem 4.4 and 4.3 we have $a_L(Q_1, Q_2) = a_L^2(Q, Q_1) = 1$. Then the result follows from theorem 4.2.

As an application of the preceding theorems we prove the following result (due to Witt and Arf). See also [2].

Theorem 4.6. *Under the assumptions of Th. 4.5, Q_1 and Q_2 are equivalent if the dimension n is 2 or 3.*

Proof: By theorem 4.5 it suffices to show that if two quadratic forms in dimensions 2 or 3 are equivalent if their Clifford algebra's or their second Clifford algebra's are isomorphic and if their discriminants are equal. This amounts to finding Q from $C(Q)$ or $C^+(Q)$, if $\Delta(Q)$ is given.

We distinguish several cases.

(a) $n = 2, \chi(K) \neq 2$. Take an orthogonal basis (e_1, e_2) of E such that $Q(\xi_1 e_1 + \xi_2 e_2) = \alpha_1 \xi_1^2 + \alpha_2 \xi_2^2$. The Cliffordalgebra $C(Q)$ is a generalized quaternion algebra ([4]), having a basis $(x_i)_{0 \leqslant i \leqslant 3}$, x_0 being the unit element, with multiplication rules
$$x_1^2 = \alpha_1,\ x_2^2 = \alpha_2,\ x_3^2 = -\alpha_1 \alpha_2, \quad x_i x_j + x_j x_i = 0 \qquad (i \neq j).$$

The norm of an $x=\sum_0^3 x_i$ of $C(Q)$ is $N(x)=\xi_0^2-\alpha_1\xi_1^2-\alpha_2\xi_2^2+\alpha_1\alpha_2\xi_3^2$. N is a quadratic form equivalent to Q_1-Q, where Q_1 is the restriction of N to the subspace spanned by x_0 and x_3. But Q_1 depends only on $\Delta(Q)=\alpha_1\alpha_2$, hence by Witt's theorem the equivalence class of Q is fixed once N and $\Delta(Q)$ are given.

(b) $n=2$, $\chi(K)=2$. The argument in this case is quite similar to that just given.

(c) $n=3$. Here only the case $\chi(K)\neq 2$ has to be considered (since a quadratic form with a nondegenerate bilinear form over a field with characteristic 2 has an even dimension).

We shall show now that the equivalence class of Q is determined by $\Delta(Q)$ and the second Clifford algebra $C^+(Q)$. Take an orthogonal basis (e_i) of E such that $Q(\sum_1^3\xi_i e_i)=\sum_1^3\alpha_i\xi_i^2$. Then $C^+(Q)$ is again a generalized quaternion algebra with a basis $(x_i)_{0\leqslant i\leqslant 3}$ such that x_0 is the unit element and that $x_i^2=-d\alpha_i(1\leqslant i\leqslant 3)$, $x_ix_j+x_jx_i=0(1\leqslant i,j\leqslant 3)$, where $d=\alpha_1\alpha_2\alpha_3$. The norm $N(x)$ of $x=\sum_0^3\xi_i x_i$ is $x_0^2-d\sum_1^3\xi_i^2\alpha_i$. By Witt's theorem we find again that the equivalence class of Q is determined by $C^+(Q)$ and $\Delta(Q)$.

We shall now give a calculation of the classes $c_L(Q, Q_1)$ for suitable L, which will give the relation with the Hasse-invariants ([2]) and the invariants of Arf in the case of characteristic 2. First let $\chi(K)\neq 2$. We shall then express $a_L(Q, Q_1)$ as a product of classes of the form (α, β).

Replacing Q_1 by an equivalent form, we can find a basis (e_i) of E such that $Q(x)=\sum_1^n\alpha_i\xi^2$, $Q_1(x)=\sum_1^n\beta_i\xi^2$, where $x=\sum_1^n\xi_i e_i$. Put $\gamma_i=\alpha_i^{-1}\beta_i$, and let L be a Galois extension of K containing square roots λ_i of the $\gamma_i(1\leqslant i\leqslant n)$. We can take as t the linear transformation of E^L defined by $t(e_i)=\lambda_i e_i$.

Then $u_\sigma(e_i)=(-1)^{\varepsilon_i(\sigma)}e_i$, where $\sigma\lambda_i=(-1)^{\varepsilon_i(\sigma)}\lambda_i$ for σ in the Galois-group G. Now let s_i denote the symmetry in E^L defined by the vector e_i $\left(s_i(x)=x-\dfrac{B(x,e_i)}{Q(e_i)}e_i\right)$, then $u_\sigma=s_1^{\varepsilon_1(\sigma)}s_2^{\varepsilon_2(\sigma)}\dots s_n^{\varepsilon_n(\sigma)}$.
Since $s_i(x)=-e_ixe_i^{-1}$ in $C^L(Q)$ (see [4]), we can take as s_σ the element $e_1^{\varepsilon_1(\sigma)}\dots e_n^{\varepsilon_n(\sigma)}$ of C^L. Calculating $\alpha(\sigma,\tau)$ we obtain

$$\alpha(\sigma,\tau)=(-1)^{\prod_{i<j}\varepsilon_i(\sigma)\varepsilon_j(\tau)}\prod_{\varepsilon_i(\sigma)=\varepsilon_i(\tau)=1}\alpha_i. \tag{4.2}$$

This implies that

$$c_L(Q,Q_1)=\prod_{i<j}(\alpha_i\beta_i,\alpha_j\beta_j)\prod_{i=1}^{n}\{\alpha_i\beta_i,\alpha_i\}, \tag{4.3}$$

where the cohomology class $\{\alpha,\beta\}\in H^2(L^*)$ is defined if L contains a square root λ of α, and is the class of the cocycle f with

$$\begin{cases} f(\sigma,\tau)=\beta \text{ if } \sigma\lambda=-\lambda,\ \tau\lambda=-\lambda\\ \qquad\quad =1 \text{ otherwise}\end{cases} \tag{4.4}$$

We proceed to show that $\{\alpha,\beta\}=(\alpha,\beta)$ if both are defined. This is a consequence of well-known properties of the "quadratic norm residue symbols" (α, β), but it may also be proved easily by means of the results obtained above.

Take $n=2$, and take first $\alpha_1=\beta_1=1$, $\alpha_2=\alpha$, $\beta_2=\beta$. Then by (4.3), $c_L(Q, Q_1)=\{\alpha\beta, \alpha\}$. On the other hand, if we take $\alpha_1=\alpha_2$, $\alpha_2=1$, $\beta_1=1$, $\beta_2=\beta$, we find by the corollary to theorem 3.4 the same cohomology class. Hence

$$\{\alpha\beta, \alpha\}=(\alpha, \beta)\{\alpha, \alpha\}. \tag{4.5}$$

Taking $\beta=\alpha$, this gives $\{\alpha^2, \alpha\}=(\alpha, \alpha)\{\alpha, \alpha\}$. Since $\{\alpha^2, \alpha\}=1$ (this follows at once from the definition), we find $\{\alpha, \alpha\}=(\alpha, \alpha)^{-1}=(\alpha, \alpha)$. Hence $\{\alpha\beta, \alpha\}=(\alpha, \beta)(\alpha, \alpha)=(\alpha, \alpha\beta)=(\alpha\beta, \alpha)$, which implies that $\{\alpha, \beta\}=(\alpha, \beta)$.

We finally observe, that it follows from the definitions that $(\alpha, \alpha)=\{\alpha, -1\}$, hence $(\alpha, \alpha)=(\alpha, -1)$. This implies $(\alpha, -\alpha)(\alpha, -1)= =(\alpha, \alpha)=(\alpha, -1)$, hence $(\alpha, -\alpha)=1$.

Taking Q and Q_1 as in the beginning of this paragraph, we have proved that

$$c_L(Q, Q_1)=\prod_{i<j}(\alpha_i\beta_i, \alpha_j\beta_j)\prod_{i=1}^{n}(\alpha_i\beta_i, \alpha_i). \tag{4.6}$$

Now take all α_i equal to 1. Then

$$c_L(Q, Q_1)=\prod_{i<j}(\beta_i, \beta_j)$$

Defining the Hasse-invariant ([2]) by

$$h(Q_1)=\prod_{i\leqslant j}(\beta_i, \beta_j),$$

we have

$$c_L(Q, Q_1)=h(Q_1)\prod_{i=1}^{n}(\beta_i, \beta_i)=h(Q_1)(-1, \Delta(Q_1)).$$

Finally, from theorem 3.4 we get for arbitrary Q_1 and Q_2,

$$c_L(Q_1, Q_2)=(\Delta(Q_1), \Delta(Q_2))\, h(Q_1)\, h(Q_2). \tag{4.7}$$

(4.7) gives the relation with the Hasse-invariants.

We now consider briefly the case $\chi(K)=2$. We shall calculate $c_L(Q, Q_1)$ for the case that Q is a *hyperbolic* form, i.e. that there is a subspace F of E of dimension half that of E such that $Q(x)=0$ for $x\in F$. We can find $c_L(Q, Q_1)$ for arbitrary Q, Q_1 by means of theorem 4.4.

We may take a basis $(e_i)_{1\leqslant i\leqslant 2m}$ of E such that if $x=\sum_1^{2m}\xi_i e_i$, we have $Q(x)=\sum_1^m \xi_i\xi_{i+m}$. Replacing Q_1 by an equivalent form we may take $Q_1(x)=\sum_1^m(\alpha_i\xi_i^2+\beta_i\xi_i\xi_{i+m}+\gamma_i\xi_m^2)$, where $\beta_i\neq 0$ $(1\leqslant i\leqslant m)$.

First consider the case $m=1$. We may assume that $\alpha_1\neq 0$, otherwise Q and Q are equivalent, and $c_L(Q, Q_1)=1$ for all L. Now let L be a Galois extension of K containing roots λ, μ of the separable polynomial

$\alpha_1 T^2+\beta_1 T+\gamma_1$. It is easily verified that we may take for t the linear transformation defined by

$$\begin{cases} t(e_1)=\alpha e_1+e_2 \\ t(e_2)=\alpha\lambda e_1+\mu e_2. \end{cases}$$

It follows that $u_\sigma=1$ if $\sigma\lambda=\lambda$ and

$$\begin{cases} u_\sigma(e_1)=\alpha_1^{-1}\, e_2 \\ u_\sigma(e_2)=\alpha_1\, e_1, \text{ if } \sigma\lambda\neq\lambda. \end{cases}$$

We may then take

$$\begin{cases} s_{u_\sigma}=1 & \text{if } \sigma\lambda=\lambda \\ s_{u_\sigma}=\alpha_1\, e_1+e_2 & \text{if } \sigma\lambda\neq\lambda, \end{cases}$$

which gives us

$$\begin{cases} \alpha(\sigma,\tau)=\alpha_1^{-1} \text{ if } \sigma\lambda\neq\lambda,\ \tau\lambda\neq\lambda \\ \qquad\quad =1 \quad \text{otherwise} \end{cases}$$

Call the corresponding cohomology class $\langle\alpha_1, \frac{\alpha_1\gamma_1}{\beta_1^2}\rangle$. Then $\langle\alpha,\beta\rangle$ is the class $c_L(Q, Q_1)$ with Q as above and with $Q_1(x)=\alpha(\xi_1^2+\xi_1\,\xi_2+\beta\xi_2^2)$. We put $\langle 0,\beta\rangle=1$.

It follows from the definitions that

$$\langle\alpha_1\,\alpha_2,\beta\rangle=\langle\alpha_1,\beta\rangle\,\langle\alpha_2,\beta\rangle, \tag{4.8}$$

that $\langle\alpha,\beta\rangle$ depends only on the class of α modulo squares, and on the class of β modulo elements of the form $\mathscr{P}(\lambda)=\lambda+\lambda^2$. It is then easily seen that in the general case, considered in the beginning, we get

$$c_L(Q, Q_1)=\prod_{i=1}^{m}\langle\alpha_i, \frac{\alpha_i\gamma_i}{\beta_i^2}\rangle.$$

This invariant was found by Arf in terms of algebra classes ([1]). As to the cohomology class $\langle\alpha,\beta\rangle$, we remark that besides (4.8) we also have

$$\langle\alpha, \beta_1+\beta_2\rangle=\langle\alpha,\beta_1\rangle\,\langle\alpha,\beta_2\rangle, \tag{4.9}$$

which may be proved by showing that the quaternary quadratic forms

$$\alpha(\xi_1^2+\xi_1\,\xi_2+\beta_1\,\xi_2^2)+\alpha(\xi_3^2+\xi_3\,\xi_4+\beta_2\,\xi_4^2) \text{ and } \alpha(\xi_1^2+\xi_1\,\xi_2+(\beta_1+\beta_2)\xi_2^2)+\xi_3\,\xi_4$$

(expressed in the components with respect to some basis) are equivalent.

Appendix. We have used the following

Theorem. *Let A be a finite dimensional associative algebra with unit element 1 over the field L and assume that we have a finite group G of automorphisms of A, obtained by extension to A of a finite group of automorphisms of $L1$. Then if (a_σ) is a system of elements of the multiplicative group A^* such that $a_{\sigma\tau}=\sigma a_\tau\cdot a_\sigma(\sigma,\tau\in G)$, there is an $a\in A^*$ with $a_\sigma=\sigma a^{-1}\cdot a$.*

Proof. We assume of course that the unit element ε of G operates on A as the identity. The $\sigma \in G$ induce automorphisms of L. Taking $\sigma = \varepsilon$ in the relation $a_{\sigma\tau} = \sigma a_\tau \cdot a_\sigma$ we find $a_\varepsilon = 1$. Now form with variables $x_\sigma (\sigma \in G)$ an element $\sum_{\sigma\in G} x_\sigma a_\sigma$. The norm of this element with respect to L is a polynomial in $L[x_\sigma]$ which is not identically zero (take $x_\varepsilon = 1$ and the others zero), hence by the algebraic independence of the restrictions to L of the $\sigma \in G$, we can find $\lambda \in L$ such that $a = \sum_{\sigma\in G} (\sigma\lambda) a_\sigma$ has a norm $\neq 0$, hence has an inverse in A. It follows easily that $a_\sigma = (\sigma a)^{-1} a$. If L is a Galois extension of a field K with group G, and if A is the algebra of all invertible $(n \times n)$-matrices over L, this theorem reduces to a result of Speiser [5].

University of Utrecht

REFERENCES

1. ARF, C., Untersuchungen über quadratische Formen in Körpern der Charakteristik 2 (Teil I). Journal f.d. reine und angewandte Mathematik **183**, 148–167 (1941).
2. BUZBY, B. and G. WHAPLES, Quadratic forms over arbitrary fields, Proc. Am. Math. Soc., **9**, 335–339 (1958).
3. CHEVALLEY, C., The algebraic theory of spinors, New York 1954.
4. DIEUDONNÉ, J., La géométrie des groupes classiques, Berlin 1955.
5. SPEISER, A., Zahlentheoretische Sätze aus der Gruppentheorie, Math. Zeitschrift **5**, 1–6 (1919).
6. WITT, E., Theorie der quadratischen Formen in beliebigen Körpern, Journal f.d. reine und angewandte Mathematik, **176**, 31–44 (1937).